

BEST AVAILABLE COPY

Application/Control Number 10/092,074 Maginas

Response date 8/11/2004 to Notice of Informal or Non-Responsive Amendment dated 6/24/2004

Amendments to the Specification

Please replace paragraph [0009] with the following amended paragraph:

[0009] Many patents were issued teaching the use of punchcards to direct telephones to dial a certain number, as in 2,505,069 (H. C. Savino, 4/25/1950); 3,124,659 (E. R. Andregg, 5/10/1964); 3,194,893 (C. C. Auel, 7/15/1965); 3,514,549 (J. D. Askew, 5/26/1970); and 4,817,13[[6]] 5 ([[R. M. Rhoads]] J. J. Winebaum, 3/28/1989). However, those inventions did not teach that the card directing a telephone to dial a certain number would communicate a specific message upon creation of the telephonic contact.

Please replace paragraph [0013] with the following amended paragraph:

[0013] Some inventions teach the use of data on one card to allow use of a telephone and other cards, or buttons, that designate certain items to be ordered through that telephone from a distant supplier, as in 4,897,865 (A. Canuel, 1/30/1990); 4,682,014 (T. Iwama, 7/21/1987); and 6,014,430 (P. J. Gosney, 1/11/2000). Others use the reading of a sequence of one-dimensional bar codes to enter the telephone number, the holder's ID, then the items to be ordered, as in 5,465,291 (J. Barrus, 11/7/1995); 6,144,848 (J. F. Walsh, 11/7/2000); and 6,230,790 B1 (J. F. Walsh, 5/15/2001). In those inventions, there is no single card that bears both the data required to direct another apparatus to contact a recipient, and the data to place an order.

Please replace paragraph [0014] with the following amended paragraph:

[0014] As with prior cards on which machine readable data is encoded, there is moreover no express denomination, or labeling, that the card bears a full disclosure, rendered in human readable data or indicia, of all machine readable data on that same card. One-dimensional bar codes, on occasion, only disclose all machine readable data, but that disclosure is not labeled as such. Bar code data disclosures generally include codes to

start and stop the machine reading the bar code in the form of asterisks or quotation marks; see [[HTML file entitled]] "Bar Code Mechanics" [[available at www.snx.com/faq/html]], 1/28/2002. Magnetic ink character recognition (MICR) codes display various characters on the ordinary bank check, but not all in characters that are human readable or reproducible; see HTML file entitled "A Brief Introduction to MICR Technology" [[available at www.mydataflo.com/wt_s6.asp]], 1/28/2002. The flux of a magnetic particle on a magnetically sensitive plastic stripe is not visible to the unaided human eye.

Please replace paragraph [0020] with the following amended paragraph:

[0020] Many patents describe cards bearing integrated chips that enable dialing of many telephone numbers, or holding extensive other data, as in 4,900,902 (K. Sakakibara, 2/13/1990). Patent 4,817,135 ([[R. M. Rhoads]] J. J. Winebaum, 3/28/1989) teaches use of an integrated chip to generate dial tones to dial a telephone number, but no message is conveyed to the person answering the telephone call. Cards that reveal a portion of the machine readable data in variable displays such as thermal sensitive film, as in 5,932,869 (S. Gottlich, 8/3/1999), do not teach that all machine readable data borne in the card is ever revealed to the card holder or card user. In fact, prevention of the reading and reproduction of the machine readable data is seen as a means to prevent fraud, as in 5,834,756 (J. Gutman, 11/10/1998). Patent 4,677,657 (M. Nagata, 6/30/1987) teaches that a card with imbedded chips can transform an audible signal into tones that can be sent to another similar card. However, the digital message is not disclosed in human readable data, is not fixed, is not useable by third parties, and can only be received and decoded by similar cards. The method disclosed by patent 4,491,725 (L. E. Pritchard, 1/1/1985) involves use of a card where security concerns dictate concealment of medical data, which data is not fixed, which requires an immediate response to effect its purpose, and requires input of treatment codes in addition to the machine readable data of the card.

Please replace paragraph [0021] with the following amended paragraph:

[0021] Some patents describe methods to relay information, such as purchase receipts from cellular or retail point of sale devices, but do not teach that the message from a single card would alone bear sufficient data to convey both the complete message as well as the address of the intended recipients. Those patents include 5,719,918 (B. Serbetciouglu, 2/17/1998); 6,064,990 ([P. J. Gosney] K. S. Goldsmith, 1/11/2000); 6,067,529 (D. Ray, 5/23/2000); and 6,185,542 (J. C. Moran, 2/6/2001). Other methods, as in 4,229,794 (C. E. Foster, 10/21/1980), combine data from a magnetic stripe with other data about a product, to issue a label combining the two to the holder or user of the card. Such data is not fixed nor is machine readable data fully disclosed on the card; no intended, distant recipients are noted in the machine readable data nor in the human readable data; and the machine readable data on the card must be supplemented by other data regarding product weight. If machine readable data were fully disclosed on the product card and there were a price change, the user would be misled as to the function of the product card.

Please replace paragraph [0025] with the following amended paragraph:

[0025] As to the institution that makes such cards, those added features are designed to give each card holder control over the functions to be accomplished by the card and over the method actuated. That control necessarily requires that third parties (such as a retail store clerk) do not know the entire content of the machine readable data upon the card. It is the card holder's option to reveal a PIN number, address, or other data, in order to require the card maker and the third party to fulfill agreements such as provision of funds or access to a site on the terms chosen by the card holder. See "A New Credit Card Scam", Time, June 5, 2000, pp. 54-55. More recently, this trend has accelerated with privacy concerns that have led to an increase in the complexity of features meant to be solely within the card holder's control and knowledge. All of those features, and the increase of data capacity of integrated circuit (IC) chips, have rendered impossible the full disclosure of data or functions of each card.

Please replace paragraph [0027] with the following amended paragraph:

[0027] In addition, there are many duties the card maker can fulfill only by an exercise of discretion after data is received from a card holder. There are numerous situations where an institution can provide a service only when it can allow a certain time to elapse before to deciding how to respond to a request, such as a claim for insurance coverage after an auto accident, and where a third party is needed to transmit information to the institution. Current trends are toward reducing the time allowed to an institution to respond, and placing greater immediate control in the hands of the customer, an approach following a different path from this invention. Such trends increase the time and energy costs for the customer, who must spend long periods on a telephone awaiting audible prompts and entering information. See HTML file entitled "Making Contact: Virtual Call Centers Zero in on Customer and Enterprise Needs", [[available at www.cisco.com/warp/public/s_fea_how_001/article_prt.html, 3/16/2001]]. The institution, or repository of information, operated by the card maker cannot effectively utilize cards to aid in transmission of information or guarantee insurance coverage when the functions of the card are solely within the card holder's control. Moreover, communication in such situations can be greatly eased by devices that allow the card holder to repetitively transmit messages to the institution that will then decide whether, and how, to take action in a series of similar circumstances. Energy costs can also be reduced by allowing issuance of fixed messages without a need for lengthy telephone contact.

Please replace paragraph [0037] with the following amended paragraph:

[0037] The combination of commands and data upon the machine-readable memory are sufficient to reconfigure a standard unmodified point of sale device, a communication device, other data readers, and associated computer devices to transmit the message or messages, [[in]] the encoded machine readable content of which was previously disclosed in human readable data, along with additional optional data, to the central computer of the card maker or its agents. The software and/or data in the central computer then

would be reconfigured and result in transmission of the appropriate message and data to the card maker, its agents or to persons other than the user of the Message Card.

Please replace paragraph [0040] with the following amended paragraph:

[0040] The ordinary credit card reader 402 is a device comprised of a magnetic head and electronic circuitry in a cabinet. The machine readable data, if on a magnetic stripe, may conform to American National Standards Institute (ANSI) or the International Organization for Standards (ISO) standards and configurations widely adopted as common within the industry, such as those at ISO/IEC 7811 et seq., as are well known to those of ordinary skill in the art. Such standards may be obtained from ANSI at 11 W. 42d St., 13th Floor, New York, NY, 10036, USA. Standards of other industry organizations, both in the U.S.A. and abroad, such as those of the American Bankers Association in its use of Bank Identification Numbers to facilitate current uses of credit cards, also enable one with ordinary skill to make the invention. A general description of magnetic encoding can be found at the HTML file entitled "ID Tech's Guide to Magnetic Encoding on Cards", [[available at www.idt-net.com/magnetic/index/cfm]], January 22, 2002.

Please replace paragraph [0050] with the following amended paragraph:

[0050] There is no need to disguise or encrypt the message transmitted by the machine readable memory of the Message Card, so that the human readable data can fully disclose the machine readable data. Disguise or encryption on the ordinary credit card, access card or other devices comprising substrates with machine readable memories help identify the card holder as the unique individual who has the authority to execute a contract with the card maker. As mere use of the Message Card results in no execution of a contract between the card holder and the card maker, the disclosure of all data does not limit the function of the Message Card nor harm any card holder or card maker. Thus, not only may the machine readable data, in alphanumeric characters or ASCII or other means ordinarily known to those skilled in the art, be fully displayed in human readable

data upon same substrate, but the Message Card may be [[pierced by an aperture and then]] suspended in full public view, perhaps from a vehicle mirror, in furtherance of the intended use of the functionally descriptive material. Even if no machinery is available to read the machine readable data, the full disclosure would permit reproduction of that transmission by use of a computer keyboard or telephone keypad to enter the disclosed data. Other elements of ordinary credit cards and access cards that are not necessary for the effective functioning of the Message Card are those which act as tokens to signify the card holder's identity or authority to use the card, such as the signature blank, the embossed name of an individual, or common holographic devices meant to prevent counterfeiting.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.